Pewne rzeczy 2

Edycja techniczna

współudział

Spis treści

3. Podstawy podstaw – Zanim choćby pomyślisz o Signalu (dodatek techniczny)

3.4. Podstawy działania telefonów komórkowych i sieci GSM

Telefon komórkowy jest dość nową technologią. Podstawowe założenia telefonii komórkowej zostały ustalone w latach 80. XX wieku, czyli już w dobie „antyterroryzmu", ciężkiego ataku państwa na społeczeństwo i masowej inwigilacji. Właściwie to wszystko wskazuje na to, że telefony komórkowe były wykorzystywane przez służby jako podsłuchy zanim na dobre pojawiły się w popkulturze, a już na pewno zanim pierwsze egzemplarze dotarły do p*lski. Cała architektura sieci komórkowej opiera się na założeniu, że anonimowość jest groźna. Ważne do rozróżnienia są trzy nazwy:

- Numer MSISDN – to jest to, co zwykle nazywamy numerem telefonu. Wbrew pozorom nie jest on zbyt ważny z punktu widzenia inwigilacji i łatwo go zmienić.
- Numer IMSI – to unikatowy numer karty sim, coś jak jej numer rejestracyjny (nie jest tożsamy z numerem MSISDN i dla danej karty sim jest niezmienny).
- Numer IMEI – to unikatowy numer aparatu telefonicznego, coś jak jego numer rejestracyjny (nie jest tożsamy z numerem MSISDN, ani ISIM i nigdy się nie zmienia).

Zawsze gdy włączasz i wyłączasz telefon, a także gdy wysyłasz SMSa lub gdy gdzieś dzwonisz, a także gdy ktoś dzwoni do ciebie, to telefon loguje do sieci parę numerów ISIM i IMEI wraz z twoją dokładną lokalizacją. Operatorzy są zobligowani przechowywać te dane przez 12 miesięcy, a jeśli zostanie wszczęte postępowanie to w nieskończoność. Służby mają do tych danych natychmiastowy dostęp, bez pisania wniosków i bez żadnej kontroli. Dokładnie rzecz biorąc to w każdej komendzie wojewódzkiej p*icji pracuje zespół p*icjantów, którzy mają upoważnienie komendanta do sięgania po te dane, kiedy tylko uznają to za stosowne, a operatorzy komórkowi udostępniają im je bez pośrednictwa własnego personelu. Po prostu p*icjanci widzą te dane w specjalnie udostępnionych im do

tego bazach. Operatorzy telefonii komórkowej są do tego zmuszeni z mocy ustawy i zwykle zatrudniają byłych p*icjantów po to, żeby przepływ informacji był sprawny i aby p*icja była zadowolona, bo nie chcą mieć problemów z prawem.

I tak, to prawda, da się włączyć zdalnie mikrofon w telefonie. A mikrofony w nowych telefonach są naprawdę czułe. Nie sądzę, żeby służby przed erą telefonii komórkowej miały dostęp do lepszych podsłuchów. Słyszałxm kiedyś jak ktoś dobrze znający się na temacie mówił, że telefon to urządzenie szpiegowskie z funkcją dzwonienia.

3.5. Podstawowe informacje o śladach jakie zostawiamy w internecie

3.5.1. Numer IP

Tu znowu będzie chwilę o numerach. Najważniejszym śladem jaki zostawiasz w sieci i który właściwie jest publiczny, to numer IP. Do numeru IP ma dostęp każdy operator strony, którą odwiedzasz. Każda osoba administrująca blogiem, skrzynką pocztową, forum internetowym, portalem informacyjnym czy Facebookiem widzi dokładnie co robią jej użytkownicy. W logach widoczne są akcje typu pisanie komentarzy, wysyłanie maila itp. w połączeniu z numerem IP. Numer ten od razu (to również informacje publiczne, coś jak w wypadku tablic rejestracyjnych) wskazuje na dostawcę usług internetowych (np. Orange, UPC czy coś takiego) i przybliżoną lokalizację. To właśnie dostawca usług internetowych nadaje IP i jest w stanie powiązać to dokładne IP z „punktem odbioru" i numerem umowy, czyli z czyimiś danymi. Jeśli przyjdziesz z laptopem do znajomej osoby i połączysz się z jej siecią wifi, operator sieci nada ci numer IP, ale nie będzie tak od razu wiedzieć, że to ty. Będzie wiedzieć na czyje dane zawarta jest umowa na punkt odbioru z którego się łączysz, a jeśli to internet mobilny, to gdzie obecnie znajduje się karta sim. P*icjanci, jeśli zainteresują ich działania podjęte z jakiegoś IP (np. mail z groźbami), będą w stanie znaleźć się w odpowiedniej lokalizacji, nie w ciągu dni, a w ciągu minut.

3.5.2. Numer MAC

Innym numerem ważnym z punktu widzenia opsec jest numer MAC. MAC to numer fizyczny karty sieciowej, znowu trochę jak numer rejestracyjny laptopa czy komórki i wiążą się z nim dwie dobre wiadomości. Po pierwsze numer MAC nie wychodzi z sieci lokalnej, tzn. jeśli łączysz się z routerem koleżanki i robisz pewne rzeczy, to p*cjanci najpierw przyjadą do niej, a dopiero później będą szukać na routerze numerów MAC urządzeń, które łączyły się z siecią. Numer MAC nie jest widoczny dla administratorek stron, które odwiedzasz, one dostają tylko IP. Druga dobra wiadomość jest taka, że numer MAC łatwo zmienić. Stąd w starych dobrych czasach, gdy dużo było słabo zabezpieczonych sieci wifi, osoby hakerskie po prostu włamywały się do nich ze zmienionym adres MAC i wykonywały swoje zajęcia, zostawiając w sieci adres IP wskazujący tylko na ofiarę włamania, nie zaś na osobę

włamującą się. Jak już ktoś dotarł nawet do routera, to jedyne co tam znalazł to adres MAC, który był za każdym razem inny, nie miał więc żadnej wartości dowodowej. Nie zmienia to faktu, że wiele takich osób wpadało głupio np. googlując swoje imię i nazwisko w czasie gdy łączyły się z takiej złamanej sieci.

3.5.3. Cyfrowy odcisk palca

Jak widzisz, gdyby problemem było tylko IP to miałybyśmy już kilka ciekawych pomysłów na postanie anonimowx i całkiem sporo przestrzeni na kreatywność. Publiczne sieci wifi, np. na uniwersytetach zwykle wymagają wprawdzie podania jakichś danych, ale są łatwymi celami dla początkujących osób hakerskich, choć warto pamiętać o wszechobecnym monitoringu. Tam, gdzie jest wifi, zwykle sięga też jakaś kamera. Natomiast śledzenie w internecie to nie tylko zajęcie służb, ale przede wszystkim gigantyczny zysk dla korporacji sprzedających wirtualne powierzchnie reklamowe. Dlatego korporacje starają się identyfikować użytkowników na podstawie dziesiątek rzeczy i naprawdę cały czas pracują nad tym, żeby robić to lepiej. To z jakiego systemu operacyjnego się łączysz, z jakiej przeglądarki, z jakiego urządzenia, jaka jest przekątna twojego ekranu, jakie masz zainstalowane dodatki i masa innych danych - to wszystko jest widoczne i analizowane. Śledzące piksele i ciasteczka zawierają dane o witrynach, jakie ostatnio odwiedzałxś, o stronach na jakie jesteś zalogowanx - a przez to też mają twoje dane osobowe. Korporacje typu Google gromadzą i analizują te dane, nie ze złośliwości tylko dla zysku, sprzedając później „profil reklamobiorcy", czyli twoją uwagę, reklamodawcom. Telefony komórkowe zaś pozwalają zbierać o tobie jakieś trudne do ogarnięcia dane, w stylu tego jak często chodzisz do kibla i czy śpiąc sięgasz po komórkę. Osobną kwestią są tak zwane urządzenia bliskiego pola, czyli urządzenia, które nie mając dostępu do internetu łączą się z telefonami i komputerami przez bluetooth. Obecnie te urządzenia są jednym z głównych obszarów badawczych Amazona. Pozwalają zbierać jeszcze więcej danych o tobie, aż do sporządzania mapy twojego domu włącznie, tylko po to, żeby móc zaoferować ci bardziej dopasowaną reklamę. Cyfrowy odcisk palca jest zwykle tak charakterystyczny, że korporacje potrafią cię po nim bezbłędnie rozpoznać. Dlatego sama zmiana MAC i IP nic nie daje. Zresztą masz także unikatowy styl wypowiedzi i nawet tempo uderzania w klawisze identyfikuje cię bezbłędnie to się nazwywa keystroke dynamics.

O tym jak zaopiekować się tymi problemami będę pisać w dalszej części zina. Na razie chcę tylko, żebyś odłożyłx telefon i komputer. Po prostu najpierw wyobraź sobie działania bez nich, by potem ewentualnie do nich wrócić, jeśli tak zdecydujesz.

4. Jak działają nasi przeciwnicy (dodatek techniczny)

4.3. Rozpoznanie internetu

Jakkolwiek absurdalnie by to nie brzmiało to w każdej komendzie wojewódzkiej p*icji istnieje grupa p*icjantów, którzy w trybie 24/7 monitorują internet. Ich formalna nazwa to pion rozpoznania w dziale ds. cyberprzestępczości. Ci p*icjanci nie zajmują się wcale żadną „cyberprzestępczością" tylko przeglądają media społecznościowe, fora, działy komentarzy itp. w poszukiwaniu interesujących treści. Mają oni upoważnienia do tego by sięgać po dane telekomunikacyjne, czyli np. sprawdzać adresy IP (patrz rozdział 3.4.1) z których pochodzą określone wpisy i czasem reagują natychmiast wysyłając pod właściwy adres fizyczny patrole p*icji, lub przekazują sprawy do dalszego badania przez inne jednostki p*icji.

Zwłaszcza wydziały prewencji zajmujące się pacyfikacją protestów (czyli w ich żargonie „zabezpieczaniem zgromadzeń") chętnie korzystają z pracy pionów rozpoznania. Dzięki temu prewencja może ocenić, ilu funkcjonariuszy zaszeregować do pacyfikowania danego protestu, jak ich wyposażyć i jaką przyjąć taktykę.

6. Trochę techniki

6.1. Generalne zasady bezpieczeństwa urządzeń elektronicznych

6.1.1. Zarządzanie hasłami

Jeśli już naprawdę chcesz używać elektroniki do wrażliwej działalności, pomimo ryzyka, o którym pisałxm w rodziale 3.3., to będziesz potrzebować przynajmniej kilku haseł. Zresztą, niezależnie od tego jak potoczą się twoje losy, to jeśli masz zapamiętać tylko jedną informację dotyczącą technicznego opsec, to niech brzmi ona tak:

Do każdej usługi, strony internetowej, aplikacji itp. musisz mieć inne, zupełnie unikatowe hasło, o długości przynajmniej kilkunastu znaków. Idealne hasła są niesłownikowe, czyli nie brzmią jak żadne wyrazy zrozumiałe dla ludzi.

To rzecz jasna nastręcza pewnych kłopotów. W praktyce jednak prawie wszystkie hasła możesz losowo generować, a potem przechowywać w managerze haseł. Managery haseł to małe programiki, które przechowują hasła w zaszyfrowanych bazach danych. Są one łatwe i szybkie w obsłudze i przede wszystkim są dostępne na wszystkie systemy i urządzenia. Dobrym przykładem jest KeePassXC. Działa to tak, że zapamiętujesz jeszcze jedno, ostatnie hasło, do odszyfrowania bazy w managerze haseł i więcej rzeczy już nie musisz pamiętać. Zacznij używać managera haseł.

6.1.2. Aktualizacje

Mam nadzieję, że to dla ciebie oczywiste: oprogramowanie musi być aktualne. Regularne instalowanie wszystkich zalecanych aktualizacji jest podstawowym warunkiem tego, żeby twoje urządzenie nie stało się łatwym celem. Niezależnie od tego, czy chodzi tu o telefon komórkowy, czy laptopa i czy mówimy o aktualizacjach całego systemu, czy pojedynczych aplikacji, wszystko co masz zainstalowane musi być aktualne. Na szczęście minęły już czasy, gdy aktualizacje rutynowo psuły działające programy czy systemy. Jeśli program pyta czy się zaktualizować zawsze kliknij „tak”.

6.1.3. Szyfrowanie wszystkich danych

Cały dysk telefonu lub komputera, którego używasz powinien być zaszyfrowany. Właściwie dotyczy to nie tylko urządzeń, które wykorzystujesz do wrażliwych działań. Warto

zabezpieczyć również swoje zdjęcia z wakacji i dane bankowe na wypadek zupełnie zwyczajnej kradzieży urządzenia. W wypadku telefonów nie jest to problem, gdyż zarówno urządzenia z Androidem, jak i te z iOS domyślnie szyfrują całe dyski, jeśli tylko są zabezpieczone pinem lub wzorem. Dlatego zawsze należy włączyć długi pin lub skomplikowany wzór.

Jeśli wykorzystujesz komputer do wrażliwej działalności, to problem szyfrowania rozwiąże za ciebie Tails lub Qubes, opisane w podrozdziale 6.3.5. Obydwa te systemy domyślnie szyfrują wszystkie dane i korzystając z nich, nie trzeba się tym w ogóle przejmować.

Zaszyfrowanie danych na „zwykłych" systemach operacyjnych także jest możliwe. Taką opcję oferuje np. MacOS, prawie wszystkie Linuxy i Windows 10 Professional, ale niestety nie Windows 10 Home, który wciąż jest bardzo popularny. Nie będę jednak tutaj opisywać szyfrowania dysków na tych systemach, gdyż generalnie nie należy używać ich do wrażliwej działalności.

6.1.4. Zabezpieczanie urządzenia przed dostępem fizycznym

Jeśli chcesz utrudnić p*icjantom dostęp do danych w twoim telefonie, to rozsądnym wyborem jest posiadanie smartfona z Androidem lub iOS. Obydwa systemy operacyjne są domyślnie zaszyfrowane i póki nie odblokujesz ekranu, nie da się za bardzo wydobyć z nich danych. Jak już wspominałxm - ważne jest, aby telefon był zabezpieczony długim pinem lub skomplikowanym wzorem, a nie odciskiem palca. Masz prawo odmówić odblokowania telefonu, natomiast musisz się wtedy liczyć ze skonfiskowaniem go na długie miesiące. Rozumiem, że możesz tak po prostu nie chcieć by p*icjanci przeglądali dane w twoim telefonie nawet jeśli nie są one wrażliwe.

Telefon z Androidem lub iOS zabezpieczony odpowiednim pinem lub wzorem jest raczej trudny do odblokowania bez twojej wiedzy i jeśli p*icjanci go przejmą przy rutynowej kontroli, raczej nie należy się martwić, że bez twojej pomocy dadzą radę go odblokować. Natomiast, rzecz jasna, szyfrowanie nie chroni przed takimi atakami, jak te opisane w podrozdziale 6.1.6.

Przechowywanie wrażliwych danych w rozmowach na Signalu na słabo zabezpieczonym telefonie doprowadziło już w p*sce do zatrzymań osób anarchistycznych. Pamiętaj o tym, by przynajmniej mieć ustawione znikające wiadomości we wszystkich konwersacjach, na wszystkich komunikatorach, tak aby żadne dane nie były wiecznie. Warto zabezpieczyć aplikacje do komunikacji dodatkowym pinem (dobre aplikacje dają taką możliwość) tak, aby samo odblokowanie telefonu nie umożliwiało wejścia do aplikacji. O wyborze komunikatorów piszę osobno w rozdziale 6.9.

Analogicznie należy postępować z laptopami. To znaczy, że jeśli twoje wrażliwe dane są przechowywane na jakimś dysku (dysku komputera, pendrive itp.), dysk ten musi być zaszyfrowany; jeśli ktoś oprócz ciebie może w danym momencie uzyskać dostęp do laptopa, na którym pracujesz, to musi on zostać wyłączony. Wyłączaj laptopa zawsze, zanim wyjdziesz z domu i zawsze, gdy pojawia się zagrożenie kontroli.

Warto pamiętać o tym, że zarówno laptopa jak i telefon można pod twoją nieobecność rozebrać i zamontować coś w ich wnętrzu. Tak zamontowane urządzenia mogą przykładowo zbierać dane z klawiatury, podsłuchiwać cię lub śledzić twoją pozycję. Istnieją także zaawansowane ataki wykorzystujące fizyczny dostęp do laptopa tuż po tym, jak został on wyłączony, do odszyfrowania dysku i wydobycia danych (słynny „cold boot attack" – zainteresowanych odsyłam do wyszukiwarki). Oznacza to, że urządzenia, którego wykorzystujesz do wrażliwej pracy, generalnie nie należy porzucać byle gdzie.

Upewnij się, że trzymasz laptopa w trudno dostępnym miejscu, do którego nie łatwo jest uzyskać dostęp, nie zostawiając śladów (np. w dobrze zamykanej szafce w biurku). Nigdy nie udostępniaj innym osobom swojego laptopa, ani nie pozwalaj, by pałętał się niepilnowany.

Oczywiście zarówno telefon jak i laptop mają wbudowany mikrofon i kamerę. Stąd, gdy nie korzystamy z kamery, to należy ją czymś zakryć. Praktyka ta jest już na tyle popularna, że producenci komputerów zaczęli sami montować przesuwane zaślepki. Mikrofonu nie da się łatwo wymontować, stąd nie należy rozmawiać o wrażliwych rzeczach w pobliżu urządzeń elektronicznych.

6.1.5. Szyfrowana kopia zapasowa

Nierozsądnie jest trzymać wszystkie buteleczki z benzyną w jednym plecaczku, bo jak plecaczek spadnie, to wszystkie mogą się pobić. Dlatego warto mieć kopie danych, które trzymamy na naszych zaszyfrowanych systemach operacyjnych.

Pod Tailsem (opisanym lepiej w rozdziale 6.3.5.1) mamy zainstalowany program Dyski (Disks). To prosty program, który można obsłużyć za pomocą ładnego, szarego okienka z przyjemną grafiką. Używając Dysków, możesz łatwo sformatować jakiegoś pendrive'a (nie tego, na którym masz Tailsa, innego). Jeśli wybierzesz opcję „ext4" to będziesz mogłx wybrać kwadracik „Zabezpiecz dysk hasłem (LUKS)". Hasło należy zapamiętać lub zapisać w KeePassieXC. Tak oto utworzyłxś zaszyfrowanego pendrive, teraz możesz zrobić na nim kopię zapasową plików. Dobrze ją trzymać w innym miejscu niż oryginalne dane, żeby w wypadku pożaru lub powodzi chociaż jedna kopia nam została.

6.1.6. Najpierw pomyśl, zanim zrobisz

Miażdżąca większość ataków mających na celu wykradzenie danych z urządzeń elektronicznych, w tym tych dokonywanych przez służby, na jakimś etapie wykorzystuje socjotechnikę. Chodzi o wykorzystanie aktywnej współpracy ofiary ataku. Osoba atakująca zwykle podszywa się pod kogoś, kim nie jest, chcąc żebyś pobrałx plik, kilnęłx w link lub wpisałx gdzieś swoje dane logowania. Niekiedy samo przejście do podstawionej strony wystarczy, by napytać sobie biedy. Z socjotechnik korzystały p*skie służby specjalne, instalując swoim ofiarom Pegasusa, czyli program szpiegowski na telefony komórkowe. Używały jej również wiosną 2022 r*syjskie służby specjalne atakujące haktywistów chcących sabo-

tować r*syjski internet w początkach wojny w ukra*nie. Aby ustrzec się przed atakiem socjotechnicznym należy trzymać się kilku zasad:

1. Zachowaj ostrożność wobec wszystkich wiadomości, których w danym momencie nie oczekiwałxś.
2. Jako czerwoną flagę traktuj wiadomości zawierające wezwanie do pilnych działań, pod silną presją czasu (masz tylko 24h, kliknij teraz itp.)
3. Pamiętaj, że podszycie się pod kogoś - zarówno mailowo jak i esemesowo - jest dziecinnie proste.
4. Zwróć uwagę na podesłane linki. Ataki socjotechniczne często zawierają prośbę o kliknięcie w link podobny do zaufanego, ale zawierający literówkę, lub zmienioną kolejność, np. riseup.mail.net zamiast mail.riseup.net. Nie klikaj w linki skrócone, zawierające tylko ciągi losowych znaków - nie wiadomo co się za nimi kryje.
5. W razie wątpliwości, skontaktuj się z rzekomym nadawcą wiadomości INNYM kanałem - czyli nie odpowiadając na podejrzaną wiadomość, a dzwoniąc, pytając bezpośrednio, pisząc na innym komunikatorze - aby potwierdzić, że otrzymana wiadomość jest prawdziwa.

6.2. Urządzenia mobilne

Tak jak już wspominałxm w rozdziale 3.4., telefon komórkowy to nie jest największy sojusznik osób anarchistycznych. Główny problem z urządzeniami GSM to stałe, bardzo dokładne namierzanie, powiązanie z licznymi łatwo identyfikującymi danymi, a także wbudowany mikrofon i (już prawie zawsze) kamera. Właściwie, to nawet jeśli masz kartę sim zarejestrowaną na tak zwanego słupa lub też zupełnie niezarejestrowaną kartę sim, a używasz telefonu w „normalny" sposób, to bardzo łatwo można cię zidentyfikować na podstawie lokalizacji i siatki połączeń.

Kolektyw Riseup, czyli anarcho-lewicowa grupa, świadcząca usługi informatyczne dla osób anarchistycznych, opublikował na swojej stronie poradnik dotyczący urządzeń mobilnych, który rekomenduje „wysoko-profilowanym celom służb" całkowitą rezygnację z telefonów komórkowych. Nieposiadanie telefonu w ogóle jest dobrym rozwiązaniem, które polecam, bo sprzyja przypominaniu sobie wielu fajnych umiejętności.

Ewentualnie można mieć telefon i nie używać go w ogóle w żadnym, jakimkolwiek związku z wrażliwymi czynnościami. Jeśli posiadasz telefon i robisz cokolwiek związanego z akcją to zostaw go w domu, najlepiej włączony, w tym miejscu, w którym leżałby, jakbyś faktycznie byłx w domu.

Posiadanie telefonu, na którym nie mamy żadnych wrażliwych danych, sprzyja wtapianiu się w tłum (ludzie zwykle mają telefony w dzisiejszych czasach). Możesz nawet rozważyć udostępnienie zawartości tego telefonu służbom gdy zostaniesz o to poproszonx.

Warto jednak pamiętać, że smartfon to pułapka i łatwo się zapomnieć i umieścić na nim dane, których tam być nie powinno (np. robiąc zdjęcia). Przez cały czas miej też w pamięci to, że smartfon zdradza twoją lokalizację i może naprawdę skutecznie cię podsłuchiwać.

Jeśli już zamierzasz korzystać z telefonu komórkowego i dopuszczasz, że jest choć niewielka szansa, że znajdą się tam istotne dane, to niech będzie to smartfon z Androidem lub iOS, gdyż te urządzenia mają zaszyfrowane dyski. Tak zwane „cegły", czyli stare telefony mogą być z łatwością przejrzane przez p*icję przy rutynowej kontroli. „Cegły" mają tylko taką zaletę, że pewnie nie będziesz tam trzymać zbyt wielu informacji, ale często jedna wrażliwa informacja przechwycona przez przeciwnika wystarczy. Wiem, że się powtarzam, ale urządzenie z Androidem lub iOS zabezpiecz długim pinem lub skomplikowanym wzorem, a nie odciskiem palca.

Lepiej zabezpieczone są urządzenia na których sprzęt i oprogramowanie jest tego samego producenta. Dlatego dobrym wyborem jest iPhone, bo w jego wypadku Apple dostarcza zarówno system operacyjny jak i smartfona lub Google Pixel, gdyż Android jest dziełem Google. Niestety ani jedno, ani drugie urządzenie nie jest tanie, ale daje dodatkową ochronę w postaci częstych i szybkich aktualizacji systemu operacyjnego. Jeśli masz smartfona z Androidem od innego producenta niż Google, to wszystkie łaty bezpieczeństwa będą dla ciebie dostępne z istotnym opóźnieniem.

6.2.1. Burner phone

Burner phone to telefon, którego używać będziesz TYLKO w trakcie akcji. W burner phone chodzi o to, żeby tego urządzenia nigdy nie dało się powiązać z twoją oficjalną tożsamością. Oznacza to, że na ciebie nie będzie wskazywać ani historia lokalizacji tego telefonu, ani połączeń dokonywanych z jego karty SIM, ani z tego aparatu, ani historia kart SIM wkładanych do tego telefonu i tak dalej. Dobrym początkiem burner phone jest kupienie nowego aparatu telefonicznego w stacjonarnym sklepie za gotówkę i włożenie go do szuflady na kilka miesięcy, żeby sklep, w którym go kupiłxś, zdążył usunąć zapis z kamer. Pewien szpicel, który celowo chciał zostawić ślad przy transakcji zakupu telefonu za gotówkę, tak aby obciążyć swoich wspólników, nabił sobie punkty na kartę lojalnościową wydaną przez sklep. Choć płacił gotówką, to zostawienie takiego śladu wystarczyło, aby p*icja wpadła na trop zakupionego telefonu.

Trochę trudniejsze jest zorganizowanie karty SIM. Taka zarejestrowana na twoją matkę lub babcię się nie nada. W darknecie, czyli w internecie dostępnym tylko przez sieć Tor, można kupić karty SIM zarejestrowane na tak zwane słupy. Nie znam obecnych cen, ale jeszcze niedawno były one prawie tak tanie jak zwykłe startery sim. Mają one taką wadę, że nie ma żadnej gwarancji, czy i jak długo będą działać. Wszystkie karty zarejestrowane na słupa jakie widziałxm przestawały działać po jakimś czasie i nie za bardzo da się przewidzieć kiedy to się stanie. Zaletą p*skiego numeru zarejestrowanego na słupa jest to że łatwo kupić do niego doładowanie za gotówkę, również nie zostawiając specjalnie śladów. Alternatywą są cz*skie karty, których nie trzeba rejestrować wcale i można je kupić w cz*cach na stacjach benzynowych, w marketach itp. (choć w takich punktach zwykle nie

ma dużego wyboru, można udać się do salonu operatora po więcej ofert). Ich zaletą jest to, że generalnie będą działać przez z góry określony czas, natomiast trudno je doładować anonimowo nie będąc w cz*chach. Poza tym w cz*chach usługi telekomunikacyjne są droższe i gorsze niż wp*sce, a zwłaszcza oferta przesyłu danych internetowych jest znacznie gorsza niż u p*skich operatorów.

Mając już zestaw złożony z nowego telefonu i anonimowej karty sim możesz używać burner phone do map, szyfrowanej komunikacji i czego tam potrzebujesz. Aby nie dało się powiązać takiego telefonu z twoją tożsamością, nie możesz go nigdy włączać ani w swoim domu, ani w innych miejscach z których zwykle loguje się twoje urządzenie mobilne. Najlepiej włączać go jadąc na akcję w jakimś mocno uczęszczanym miejscu i wyłączać w takim samym miejscu wracając z akcji. Taki telefon może łączyć się tylko z innymi burner phone'ami.

Problem polega na tym, że taki telefon nadal posiada mikrofon, nadal loguje się do sieci i podaje swoją lokalizację, a jeśli jest smartfonem, to dodatkowo ma kamerę i GPS. Jeśli służby zorientują się, że dany numer IMEI to numer sprzętu używanego do akcji - np. zobaczywszy, że wielokrotnie logował się do sieci z miejsc „przestępstwa" - mogą go zacząć namierzać nie wiedząc nawet do kogo należy. Ostatecznie musisz też pamiętać o tym, że twój burner phone będzie miał dość charakterystyczne wzorce zachowań. Wprawdzie p*icja nie będzie wiedziała, że to ty go używasz, ale może ustalić, jaką pełni funkcję i zacząć obserwować lokalizację tego numeru, jeśli pojawi się w sieci. Samo śledzenie telefonu nie jest dla p*icji trudne. Wreszcie p*icjanici mogą też spróbować się do niego włamać i wykorzystać go jako podsłuch lub urządzenie monitorujące wizję, choć to już wymaga od nich więcej chęci.

Dlatego, jeśli wykorzystujesz burner phony, to dobrym pomysłem jest ograniczenie ich do mniej wrażliwych działań (np. używanie ich tylko przy rozpoznaniu) co zmniejszy szansę na to, że p*icja zainteresuje się danymi numerami IMEI i IMSI. Ewentualnie można je czasem zmieniać, choć to drogie rozwiązanie.

6.3. Maskowanie IP

Laptopy i komputery stacjonarne mają taką przewagę nad urządzeniami wyposażonymi w kartę SIM, że nie zostawiają w żadnej sieci dokładnej historii swojej lokalizacji. Numer MAC będący jedynym identyfikatorem laptopa zostaje tylko na punkcie dostępu do sieci (modemie lub routerze), poza tym dość łatwo go zmienić. Dlatego podstawowy problem w wypadku laptopów i komputerów to zamaskowanie twojego IP.

Tutaj warto zaznaczyć, że każde urządzenie podłączone do sieci ma numer IP, więc zarówno smartfon, tablet, jak i laptop zostawiają ślad w jego postaci w historii wszystkich stron internetowych i usług sieciowych, które odwiedzają. W wypadku komputera stacjonarnego czy laptopa po prostu nie musimy się martwić o dodatkowy problem jakim są dane logowania do sieci GSM unikalnymi numerami IMEI i IMSI.

6.3.1. Virtual Private Network (VPN)

VPN działa w ten sposób, że za pośrednictwem sieci swojego dostawcy internetu, powiedzmy Orange, łączysz się do serwera dostawcy VPNa. Twój dostawca internetu i p*icja widzi, że łączysz się z VPNem. VPN natomiast przepuszcza twój ruch przez jakiś „tunel" i wypuszcza go w innym miejscu. Gdy wchodzisz zatem na stronę internetową, powiedzmy na Facebooka, to dla Facebooka wygląda to tak jakbyś miałx adres IP należący do dostawcy VPNa, czyli powiedzmy do Riseupa. Riseup ma sporą część infrastruktury w Holandii, więc często gdy skorzystasz z Riseup VPN to twoje IP będzie wskazywało na holenderskie serwery Riseupa. Czyli Facebook zobaczy, że łączysz się z sieci VPN danego dostawcy, ale nie zobaczy już, że do Riseupa dostałxś się z Orange, i gdzie naprawdę mieszkasz. Problem polega na tym, że dostawca VPNu wie wszystko. To znaczy, że taki Riseup wie kim jesteś, jakie jest twoje prawdziwe IP i widzi, z czym się łączysz. VPN to usługa przeniesiena zaufania. To zaufanie jakie normalnie okazujesz swojemu dostawcy internetu (Orange, Netii itp.) przenosisz w dokładnie niezmienionej formie na dostawcę VPNa, czyli przykładowego Riseupa. No więc jeśli dostawca VPNa współpracuje ze służbami tak samo jak twój dostawca internetu, to na tym całym manewrze zyskujesz dokładnie tyle co nic. Jeśli p*icja skontaktuje się z twoim dostawcą internetu to dowie się że korzystasz z Riseupa, jeśli zaś pójdzie do Riseupa, to czego dowie się od niego? Ja nie wiem, ale wolę nie zgadywać. Z pewnością dostawcy VPNów są mocno monitorowani przez służby. Ich serwery to dla służb naprawdę łakome kąski.

6.3.2. VPN vs Tor

VPN ma pewne niewielkie zalety. Jeśli korzystasz z VPNa, to cały ruch z twojego urządzenia i wszystkie aplikacje łączą się przez VPNa, więc trudno o przypadkowe wyjawienie prawdziwego IP. Ściąganie torrentów przez Tora jest generalnie niezalecane, więc jeśli chcesz pobrać torrent ukrywając swoje IP, to VPN jest jedyną drogą. Co więcej, niektórzy dostawcy treści internetowych niechętnie patrzą na ruch z sieci Tor, a niekoniecznie mają takie polityki dot. poszczególnych dostawców VPN. Stąd są rzeczy, których nie da się zrobić przez Tora, jeśli już więc musisz je robić, lepiej robić je przez VPNa niż łącząc się bezpośrednio. Zastąpienie Tora VPNem to jednak zawsze znaczne potęgowanie ryzyka.

6.3.3. Tor – podstawowe infromacje

Tor działa na zupełnie innej zasadzie niż VPN, jego podstawowa zasada brzmi, że nikt nie wie wszystkiego. Gdy łączysz się z jakąś witryną internetową za pośrednictwem Tora, to zawsze po drodze przechodzisz przez trzy węzły sieci Tor, czyli przez 3 komputery. Twój ruch jest zaszyfrowany w taki sposób, że pierwszy węzeł wie wprawdzie kim jesteś, ale nie wie z kim chcesz się połączyć. Wie tylko, że ma wysłać wiadomość do kolejnego węzła. Drugi nie wie już, kim jesteś i przesyła zaszyfrowane zapytanie do trzeciego. Dopiero trzeci odszyfrowuje, dokąd kierowane jest twoje zapytanie, nie wie on natomiast skąd ono

pochodzi - czyli nie wie kim jesteś. Tor opiera się na publicznej architekturze - to znaczy CIA, NSA, różne inne organizacje terrorystyczne i ty, a także każda inna osoba może założyć swój węzeł sieci Tor i dzięki temu pomagać innym. Rzecz jasna służby bardzo chętnie wystawiają swoje węzły sieci Tor i nagrywają przechodzący przez nie ruch, ale prawdopodobnie jeszcze przez kilka – kilkanaście lat nic poważnego z tego nie wyniknie. Póki co wynikają z tego pewne problemy, których rozwiązania znamy.

Tor stanowi więc całkiem niezłe maskowanie twojego adresu IP. Administratorka strony, z którą się połączysz, zobaczy tylko, że łączysz z Tora. Dowie się o tobie tylko tego i tych rzeczy, które jej samx powiesz. W odróżnieniu zaś od usług VPN, Tor nie ma żadnego centralnego miejsca gdzie przechowywane są dane jego użytkowników. P*icja nie ma dokąd się udać by sprawdzić kto jest kto.

6.3.4. Tor Browser

Z Tora można korzystać na różne sposoby. Pierwszy i najłatwiejszy z nich to Tor Browser (TB), czyli przeglądarka, która zawsze działa tylko przez sieć Tor. TB jest głównym produktem Tor Project, czyli organizacji pozarządowej która stworzyła i rozwija Tora, a która finansowana jest głównie przez amerykkkański rząd. TB to aplikacja dostępna dla Windowsa, Linuxów, MacOS, Androida i iPhona. TB jest modyfikacją dość popularnej w swoim czasie przeglądarki Firefox. Użycie TB jest dramatycznie proste. Instalujesz ją, odpalasz i od tego momentu twoje działania wykonywane przez tą przeglądarkę są całkiem nieźle anonimizowane. Jej dodatkową zaletą jest to, że Tor Browser stara się upodobnić twój cyfrowy odcisk palca do cyfrowego odcisku palca innych osób używających Tora. Na przykład TB otwiera się w zminimalizowanym oknie, by nie dało zmierzyć się twojej przekątnej ekranu. TB domyślnie czyści historię i pliki ciasteczek przy każdym zamknięciu okna przeglądarki, aby utrudnić profilowanie cię na ich podstawie.

Zasadniczy minus TB jest taki, że TB w żaden sposób nie wpływa na resztę tego co dzieje się na twoim urządzeniu. To znaczy, że ruch internetowy z innych programów i aplikacji idzie sobie nadal tak jak wcześniej, czyli pewnie nie przez Tora. Jeśli używasz równocześnie w drugim oknie innej przeglądarki, powiedzmy zwykłego Firefoxa lub Chrome'a, to już ruch z nich nie idzie przez Tora i jest do powiązania z twoją osobą. Rodzi to przestrzeń na głupie błędy, w stylu wpisania czegoś w złe okno. Jeśli równocześnie używasz jakiejś aplikacji do czatu lub maila, to one także nie działają przez Tora. Poza tym TB nie ma żadnego wpływu na poziom bezpieczeństwa urządzenia, z którego korzystasz. Jeśli twojemu przeciwnikowi uda się przejąć kontrolę nad twoim telefonem lub laptopem za pomocą wirusa, którego pobierzesz przez zwykłą przeglądarkę lub pendrive'e, to TB w żaden sposób cię przed nim nie uchroni. Co więcej jeśli już twoje urządzenie jest zainfekowane wirusem, to również dane, które wprowadzasz przez TB są narażone na wykradzenie.

Wreszcie podstawowym warunkiem brzegowym, który należy spełnić zanim użyjemy urządzenia elektronicznego do jakichkolwiek działań wrażliwych jest to, że jego dysk musi być zaszyfrowany. I to najlepiej cały dysk.

6.3.5. Systemy operacyjne zbudowane wokół Tora

Aby rozwiązać powyżej opisane problemy stworzono systemy operacyjne na komputery stacjonarne lub laptopy, które przesyłają cały ruch internetowy przez Tora i które szyfrują wszystkie swoje dane. Oznacza to, że wszystkie aplikacje działające pod takim systemem łączą się tylko przez Tora, co minimalizuje ryzyko przypadkowego wyjawienia swojego IP przeciwnikowi.

6.3.5.1. Tails

Dobrym przykładem takiego systemu operacyjnego jest Tails, stworzony przez Tor Project. Tails powinien być twoim pierwszym wyborem. Jeśli już musisz użyć do czegoś sprzętu elektronicznego niech to będzie laptop z Tailsem, a nie smartfon, komputer z Windowsem, czy coś innego. Niestety Tails nie ma odpowiednika, którego mogłxbyś użyć na smartfonie.

Tails jest de facto hobbystycznym projektem. Obecnie nad jego rozwojem nie pracuje nikt na stałym etacie. To dość uderzające w zestawieniu z molochami zatrudniającymi dziesiątki tysięcy ludzi, typu Google, Apple czy Microsoft. Po hobbystycznych systemach nie należy się spodziewać komfortu użytkowania znanego z Androida, Windowsa czy MacOSa. Wysiłki osób rozwijających Tailsa skupiają się na bezpieczeństwie i ewidentnie aspekty wizualne i łatwość użytkowania zostają trochę w tyle. Można korzystać z Tailsa bez żadnej technicznej wiedzy, natomiast nie będzie to pewnie tak bezproblemowe doświadczenie jak w wypadku produktów wielkich firm. Po prostu potrzebna jest odrobina wyrozumiałości.

Tailsa zazwyczaj instaluje się na pendrive'ie lub karcie SD. Minimalna wymagana pojemność nośnika to 8 GB, ale muszą się tam zmieścić wszystkie dane jakie uważasz za wrażliwe, a które chcesz mieć pod ręką korzystając z komputera, większy rozmiar jest zatem generalnie lepszy. Dobrze wybrać pendrive'a wyposażonego w USB 3.0. Złącza USB 2.0 i USB 3.0 wyglądają tak samo, natomiast nowsze złącze, 3.0, jest znacznie szybsze. Jest ono już obsługiwane przez prawie wszystkie komputery, nawet te starsze, ale w obrocie nadal jest sporo dysków USB 2.0. Twój Tails będzie działał dużo lepiej jeśli dołożysz dosłownie parę złotych i kupisz pendrive'a z lepszym złączem. Warto więc przeczytać opis pendrive przed zakupem i upewnić się, że wyposażony jest on w USB 3.0.

Tails działa w ten sposób, że przy starcie komputera, zamiast odpalić system operacyjny z wbudowanego dysku twardego, odpala się zupełnie osobny system operacyjny z zewnętrznego nośnika (USB lub karty SD). Ma to między innymi tę zaletę, że Tails w ogóle nie ma dostępu do danych, które znajdują się na komputerze, nie może ich więc zepsuć. Trudno jest także włamywaczowi, który włamie się do Tailsa na przykład z zainfekowanej strony, jaką odwiedzisz działając przez Tora, dobrać się do zawartości dysku komputera. Ma on dostęp jedynie do danych umieszczonych na pendrive, na którym jest Tails. Stąd prosty wniosek, by nie trzymać na Tailsie nic, co może pomóc cię zidentyfikować.

Uruchomienie komputera z dysku zewnętrznego generalnie jest proste, ale inaczej wykonuje się je w wypadku komputerów różnych producentów i modeli. Ten krok często

nastręcza problemów początkującym, ale plus jest taki, że dla danego modelu komputera zawsze wykonuje się go tak samo, więc jeśli raz uda się ci to zrobić (możesz poprosić kogoś o pomoc), to już zawsze będziesz wiedzieć jak to zrobić. Niektóre komputery są skonfigurowane w ten sposób, że jeśli do portu USB jest podłączony pendrive, to zawsze spróbują wystartować system najpierw z niego, a dopiero potem z dysku. Jest więc nawet szansa, że jak już zdobędziesz pendrive z Tailsem, to nie będziesz musiałx nic robić oprócz włączenia komputera, aby go odpalić.

Instrukcje na temat tego jak pobrać Tailsa i zainstalować go na dysku USB znajdują się na stronie Tailsa. Moim zdaniem są one jasne, ale jeśli nigdy nie robiłxś tego wcześniej i nie lubisz takich zadań, możesz poprosić kogoś zaufanego o pomoc.

Ważną cechą Tailsa jest to, że jest on anamnestyczny. To znaczy, że domyślnie wszystkie dane, np. pliki jakie stworzyłxś, ustawienia jakie zmieniłxś itp. są kasowane przy wyłączaniu systemu. Ma to na celu minimalizację śladów, które mogą umożliwić zidentyfikowanie cię i powiązanie cię z określonymi działaniami wrażliwymi. Aby zmodyfikować to zachowanie należy po uruchomieniu Tailsa uruchomić program „Configure Persistent Storage", który na części pendrive utworzy zaszyfrowaną przestrzeń nazwaną „Persistent Volume". Pliki zapisane w tej przestrzeni przetrwają restart systemu. Tails może tam przechowywać też część ustawień użytkowniczki, ale tylko jeśli zostanie tak skonfigurowany. W Persistent Volume można np. przechowywać ustawienia dotyczące języka systemu operacyjnego, układu klawiatury, strefy czasowej itp. Wielu ustawień w Tailsie nie da się zachować pomiędzy restartami co bywa irytujące. Zwłaszcza, że Tails „zapomina" ustawienia Tor Browser, w tym takie, które poprawiają jej bezpieczeństwo, trzeba więc je wprowadzać po każdym restarcie.

Tails zawiera domyślnie zainstalowany menadżer haseł KeePassXC, którego należy używać, a także Electrum – portfel obsługujący kryptowalutę Bitcoin. Teoretycznie mogłxbyś używać Electrum do płatności w kryptowalutach, ale są fajniejsze waluty niż Bitcoin, a Electrum obsługuje tylko jego, tak naprawdę nie jest zbyt przydatne. Oprócz tego w Tailsie jest program graficzny GIMP i programy biurowe. Większość użytkowniczek Tailsa używa pewnie tylko Tor Browser.

Dużą zaletą Tailsa jest to, że domyślnie zmienia adres MAC komputera. Oznacza to, że łącząc się z Tailsa mamy „fałszywe" IP i „fałszywy" MAC. Tails także wykonuje więcej kroków niż samo Tor Browser w celu redukcji twojego cyfrowego odcisku palca. Każda osoba używająca Tailsa wygląda w sieci tak samo. Jeśli samx nie dostarczysz informacji na swój temat to bardzo trudno będzie cię sprofilować jeśli używasz Tailsa.

Tailsa także łatwo się pozbyć. Pamiętaj, że gdy p*icja przychodzi do ciebie do domu to właściwie zawsze ktoś obserwuje okna. Wyrzucanie dowodów przez okno nie jest dobrym rozwiązaniem. Natomiast małego pendrive'a można spłukać w toalecie, zjeść, spalić w palenisku lub rozwalić młotkiem. Przy odrobinie szczęścia nikt się nie zorientuje, że kiedykolwiek miałxś Tailsa.

Tutaj taka uwaga – jeśli zechcesz fizycznie uszkodzić pendrive, to tym co musisz zniszczyć nie jest obudowa ani złącze usb. Tam w środku jest taka płytka (układ scalony), ale zniszczenie tylko jej także nie usunie danych. Do tej płytki przyczepiony jest płaski, jedno-

lity kawałek kruchego materiału (zwykle ma grafitowy kolor). Na szczęście łatwo poważnie go uszkodzić już jednym uderzeniem w kant, ale najpierw trzeba się do niego dostać. Cała operacja wymaga więc kilku uderzeń młotkiem. Temperatura 200*C przez parę minut także załatwi sprawę.

6.3.5.2. Qubes OS

Qubes to system operacyjny na komputery stacjonarne i laptopy zaprojektowany tak, by odpowiadać na zdecydowaną większość współczesnych zagrożeń dla opsec. Albo inaczej, Qubes odpowiada na wszystkie znane zagrożenia, na które da się odpowiedzieć z poziomu systemu operacyjnego. Komputer z Qubes OS nadal zostaje podatny na takie dziury jak wspominany w rozdziale 3.2 Silent Bob is Silent i oczywiście nic nie jest odporne na twoje głupie błędy, ale Qubes to najbardziej pancerny system jaki obecnie jest dostępny. Qubesa nie odpala się z pendrive, instaluje się go na dysku twardym komputera i działa on jako „główny" system operacyjny na danej maszynie.

Jeśli na poważnie chcesz podejść do separacji tożsamości (patrz rozdział 6.6) i chcesz prowadzić np. dwa rodzaje wrażliwej działalności wykorzystując do każdego inną tożsamość (to jest bardzo pomocne, ale trudne, nie tylko w aspekcie technicznym!) to masz do wyboru mieć dwa osobne pendrive z dwoma różnymi Tailsami, albo użyć Qubesa. Przerobiwszy obydwa scenariusze, powiem ci, że na dłuższą metę Qubes jest dużo wygodniejszy.

Qubes ma dwie zasadnicze wady. Ma dość wysokie wymagania sprzętowe i jest wyraźnie trudniejszy w obsłudze niż Tails. Generalnie nie polecałxbym Qubes OS osobom, które nie mają istotnego doświadczenia z Linuxami. Jeśli masz w miarę współczesny komputer i czujesz się na siłach to polecam Qubes OS. W odróżnieniu od Tailsa, Qubes jest systemem ogólnego zastosowania. Pozwala on na jednej maszynie i pod jednym systemem operacyjnym wykonywać różne rodzaje działalności wrażliwej, a także naszą „oficjalną" działalność, taką jak praca zarobkowa, zachowując jednocześnie silną separację pomiędzy nimi.

Wykonując działalność wrażliwą spod Qubesa możesz korzystać np. z systemu, który dodaje losowe odstępy czasu pomiędzy wysłaniem jednego znaku z klawiatury a drugiego, co uniemożliwi zidentyfikowanie cię na podstawie tempa naciskania na klawisze. Jako że to i tak zaawansowany temat, którego tu z pewnością nie wyczerpię, to, jeśli cię zainteresowałxm, wpisz sobie w wyszukiwarkę „Qubes OS".

6.4. Tor – znane problemy i ich rozwiązania

Sieć Tor jest fajna, ale jest z nią kilka problemów. Oczywiście koncentrują się one woków miejsca wejścia do sieci Tor (nazywanego „entry guard") i wyjścia z niej (czyli „exit node").

6.4.1. Używaj mostów

Entry guard, czyli miejsce gdzie wchodzisz do sieci Tor, stanowi publiczną infrastrukturę. Oznacza to, że twój dostawca internetu (i p*icja) może łatwo zauważyć, że łączysz się z siecią Tor widząc, że łączysz się z entry guardem. W niektórych krajach Tor jest cenzurowany, tzn. operatorzy internetu celowo blokują możliwości połączenia z entry guardami. W innych krajach ruch do entry guardów jest celowo spowalniany, tak by użytkownicy nie chcieli korzystać z Tora, ale by trudno było oskarżyć rząd o cenzurę. Jeszcze gdzie indziej samo użycie Tora może być odnotowane i wciągnąć cię na jakąś listę osób do obserwacji. W p*sce w ciągu miesiąca z Tora korzysta około 30 tysięcy osób. To stosunkowo niewielka grupa. Jeśli p*icja jest na takim etapie postępowania, że może zawęzić poszukiwania np. do jednej dzielnicy i jednego kręgu społecznego, to może się okazać, że będziesz jedyną osobą w kręgu poszukiwania, która korzysta z Tora. Były już osoby wsadzane na długie wyroki tylko za to, że o określonej godzinie łączyły się z Torem (np. o godzinie o której wysłano maila z pogróżkami).

Sposobem na obejście tego problemu jest użycie mostów. Mosty to węzły sieci Tor, które powstały głównie z myślą o udostępnieniu sieci Tor w krajach, w których rząd blokuje dostęp do niej. W takich krajach jak ch*ny czy ir*n ludzie mają dostęp do zachodnich zasobów internetowych tylko przez Tora, a do Tora mogą mieć dostęp tylko przez mosty. To sprawia, że amerykkkański rząd kocha Tora i kocha mosty, hojnie finansując ich rozwój. Tor jest po prostu elementem globalnej wojny informacyjnej, a mosty są ważną bronią w tej wojnie. Ale z mostów można i powinno się korzystać wszędzie. Mosty to węzły wejściowe, które udają, że nie są węzłami sieci Tor, tylko że pełnią jakąś inną funkcję w internecie. Mosty nie są jednak idealne. Jeśli już p*icja uweźmie się na ciebie z jakiegoś powodu i naprawdę będzie chciała sprawdzić czy korzystasz z Tora czy nie, to objąwszy cię dokładną obserwacją będzie w stanie to sprawdzić, nawet jeśli używasz mostu. Jednak przy rutynowych przeglądach sieci pozostaniesz niezauważnx. Swoją drogą, zapamiętaj sobie – jeśli już znalazłxś się w kręgu podejrzanych to wpadniesz. Prędzej czy później znajdzie się jakiś dowód. Działając pod stałą obserwacją nie da się nie popełnić błędu. Jeśli jesteś już jedną z głównych osób podejrzanych w jakimś śledztwie, to twoją jedyną szansą jest zapaść się pod ziemię. Sztuka polega na tym, żeby nie znaleźć się w kręgu podjerzanych. Żeby jak najdłużej nic nie przykuwało uwagi do twojej osoby.

Mostów można używać zarówno używając Tor Browser spod „zwykłego" systemu operacyjnego, spod Tailsa jak i spod Qubesa. Z niezrozumiałych dla mnie powodów spod Tailsa jest to najtrudniejsze. Gdy już włączysz Tailsa i połączysz się z lokalną siecią internetową automatycznie uruchomi się program „Tor Connection". W tym programie musisz wybrać drugą, niedomyślną opcję „Hide to my local network that I'm connecting to Tor", czyli „Ukryj przed moją lokalną siecią, że łączę się z Torem". W następnym kroku trzeba wkleić adres mostu, który wygląda mniej więcej tak: obfs4 173.205.417.008:8443 1E6E21008C3355ABFE42C4680CB0F2B98795E656 cert=7wJV0TLN8K5mNXYVfMSRjMosQvrMcqiQgss4IXeUcvpz/eTGH69z6BkR4iDi39h8DOPyUA iat-mode=0

Powyższy adres mostu nie zadziała, jest tylko przykładowy. Aby dostać działający adres mostu odwiedź stronę:

https://bridges.torproject.org/

Adres mostu można zapisać w Persistent Volume, możesz używać tego samego mostu wielokrotnie, ale któregoś razu może się okazać, że przestał on działać. Nic nie jest wieczne, mosty też nie.

Z jakiegoś powodu łatwiejsze jest użycie mostów pod zwykłym TB (i pod Qubsem też). Pod TB wystarczy uruchamiając przeglądarkę zamiast domyślnej opcji „Launch Tor Browser" wybrać opcję „Configure" i na kolejnym ekranie kliknąć „Tor is censored in my country". To wszystko. Zawsze używaj mostów gdy łączysz się z Torem.

6.4.2. Nie łącz Tora i VPNa

Niektóre stare źródła w tym, źródła ALF i „Jolly Roger Secuirty Thread For Beginners" podają błędne informacje na temat rzekomych benefitów wynikających z łączenia Tora z VPNem. Tymczasem krótka wypowiedź w tej kwestii mogłaby brzmieć tak: „Przy użyciu Tora za pośrednictwem mostów nie ma żadnych korzyści z dodatkowego użycia VPNa, są natomiast ryzyka z tego wynikające. Tor wystarczy."[1]

To wszystko sprawia, że VPN naprawdę rzadko się przydaje. Szczerze powiedziawszy to nie pamiętam kiedy ostatnio używałxm jakiekolwiek VPNa. Tora natomiast owszem, zdarza mi się.

6.4.3. Używaj domen .onion

Drugi poważny problem sieci Tor dotyczy ostatniego węzła sieci jaki odwiedzasz, zwanego „exit node". Jeśli łączysz się ze „zwykłą" stroną internetową, mającą taki adres, jak np. szalej.xyz to po dotarciu do trzeciego węzła sieci Tor twoje zapytanie zostaje odszyfrowywane. Stamtąd przekazywane jest w odszyfrowanej formie (to już nie jest sieć Tor!) do docelowej strony internetowej. Wiąże się z tym kilka problemów.

Po pierwsze z adresów IP exit node'ów często dokonywane są ataki na strony internetowe, oszustwa itp. To sprawia, że często możemy zupełnie nieświadomie używać tego samego IP, które przed chwilą brało udział w masowym ataku na jakąś stronę. Dlatego dość często wchodząc z Tora np. na usługi Google albo Facebooka zobaczymy blokadę dla robotów, której może nie dać się przejść. Trzeba wtedy odczekać, albo użyć opcji „Nowa Tożsamość". Ogólnie używanie niektórych usług przez Tora jest uciążliwe. To mniej poważny problem.

Poważniejszy problem jest taki, że exit nody często same są czymś w rodzaju pułapki mającej na celu monitorować ruch internetowy i przechwytywać np. loginy i hasła. Na pewno duża część exit node'ów należy do amerykkkańskich agencji rządowych. Jak myślisz, po co im one? W większości wypadków przechwycenie hasła za pomocą exit node nie

[1] `https://www.whonix.org/wiki/Tunnels`

jest łatwe, należy jednak założyć, że globalne agencje szpiegowskie są w stanie skutecznie to robić. Co więcej exit node nigdy nie zna prawdziwego IP użytkowniczki, ale może próbować dowiedzieć się czegoś o tobie na podstawie danych jakie uda mu się przechwycić.

Dlatego przez Tora najlepiej jest się nigdy nigdzie nie logować. A jeśli już musisz się zalogować to należy jakoś ominąć exit node. Jest na to sposób. Jest nim użycie domeny .onion. Domena .onion to domena darknetowa.

6.5. Darknet

Darkent to internet dostępny tylko przez Tora. Jeśli łączysz się ze stroną za pomocą domeny .onion to nigdy nie wychodzisz z sieci Tor, ruch jest przez całą drogę zaszyfrowany i nie ma żadnego exit node, który może go przechwycić.

Ciekawostka jest taka, że Facebook od dawna ma domenę .onion: `facebookwkhpilnemxj7asaniu7vn`

Oczywiście przesyłanie swoich danych osobowych korporacjom jest złym pomysłem. Zarówno przez Tora jak i nie przez Tora.

Przeciwieństwem darknetu jest clearnet. Zatem domena clearnetowa Facebooka to facebook.com, a darknetową masz powyżej. Darknetowa jest dostępna tylko przez Tora i to bez pośrednictwa exit node'ów.

Są takie strony jak Facebook, które posiadają adres clearnetowy i darknetowy. Są natomiast strony dostępne tylko w darknecie. Darknet to wspaniałe miejsce ponieważ można tam nie tylko odwiedzać, ale także opublikować stronę internetową całkowicie anonimowo. Oznacza to, że można np. w miarę bezpiecznie otworzyć forum na którym można handlować „nielegalnymi" rzeczami, a nawet zlecać i oferować „nielegalne" usługi.

Aktualna lista popularnych stron w darknecie znajduje się pod (clearnetowym) adresem: `https://onion.live/`

6.6. Mamy nowych znajomych! - Anonimowość, pseudonimowość i separacja tożsamości

6.6.1. Anonimowość i pseudonimowość

Warto rozróżnić dwa zbliżone pojęcia: anonimowość i pseudonimowość. Anonimowość osiągasz wtedy gdy prowadzisz działania nie zostawiając żadnych danych, które można powiązać z jakąkolwiek tożsamością. Jeśli powiesz lub zrobisz coś i w ogóle się pod tym nie podpiszesz, ani nie zostawisz niczego co wskazuje na jakąś osobę bądź grupę, to jesteś anonimowx. To w gruncie rzeczy wielki, ale rzadki przywilej.

Podobnym zjawiskiem jest pseudonimowość. Pseudonimowosc polega na posługiwaniu się pseudonimem, a więc na zostawianiu śladów, wskazujących na jakąś tożsamość, która jednak jest różna od naszej „oficjalnej" („skazywalnej"?) tożsamości, czyli od danych pod

którymi widniejemy w państwowych rejestrach i pod którymi można nas skazać. W wypadku pseudonimowości pytanie brzmi, czy są takie cechy twojej tożsamości pseudonimowej, które można powiązać z twoją tożsamością „skazywalną"?

Kiedy posługujesz się pseudonimem spotykając się z kimś fizycznie to taką cechą, którą można połączyć z twoją skazywalną tożsamością jest twój wygląd, ale także chociażby ton i barwa twojego głosu czy sposób mówienia. W wypadku krótkich interakcji można jeszcze starać się zmodyfikować te cechy, ale przy spotkaniach dłuższych niż kilkanaście minut sprawa staje się trudna. Możesz co najwyżej starać się utrudnić identyfikację, ale raczej nie zdołasz jej uniemożliwić.

Wyobraź sobie taką sytuację: działasz w grupie posługując się pseudonimem. Po jakimś czasie grupa kończy działanie (lub z niej odchodzisz). Kilka miesięcy później p*icja chce przeanalizować działania tej grupy dysponując tylko zeznaniami jednego kapusia, który będzie z pamięci przywoływać fakty dotyczące twojej osoby. W takim scenariuszu masz szansę pozostać w ukryciu. Jeśli informacje, które posiada na twój temat ów kapuś są mało charakterystyczne i nie zawierają danych, które są do odnalezienia w oficjalnych rejestrach, być może nie uda się ciebie zidentyfikować.

Jednak jeśli rozpracowywanie grupy odbywa się w czasie, w którym w tej grupie działasz, to dokładne zdjęcia twojej twarzy wykonane z ukrycia raczej wystarczą aby cię zidentyfikować. Jeśli to nie przyniesie rezultatu, p*cjanci mogą cię także śledzić, by sprawdzić gdzie mieszkasz, namierzać twój telefon, lub po prostu cię wylegitymować pod byle pretekstem.

Dlatego pseudonimowość jest dużo bardziej skuteczna wtedy gdy możesz wyeliminować czynniki fizyczne, to znaczy gdy komunikujesz się zdalnie. Taką właśnie, zdalną komunikację, będę mieć na myśli, pisząc ten podrozdział. Niemniej, możesz traktować pseudonimowość jako dodatkowe, dość słabe, ale zawsze, zabezpieczenie także w innych kontekstach.

6.6.2. Tworzenie tożsamości

Tworzenie tożsamości, którą powiążesz ze swoim pseudonimem przypomina trochę tworzenie postaci w grze RPG. Twoja postać/tożsamość wykonująca działania wrażliwe może znać się na trochę innych rzeczach, niż twoja „skazywalna" tożsamość. Zwłaszcza może znać się na rzeczach, do których twoja skazywalna tożsamość nigdy się nie przyznaje. I nie musi wypowiadać się o rzeczach, na których zna się dobrze twoja skazywalna tożsamość. Twoja tożsamość może być rozwijana przez jakiś czas, a potem możesz bez żalu ją skasować, tak by zgubić wszystkie tropy. I zacząć budować nową, gdy uznasz, że zajdzie taka potrzeba.

6.6.3. Separacja tożsamości – na co zwrócić uwagę

To, co może sprawić, że zostaniesz zidentyfikowanx to oczywiście użycie jakichkolwiek danych powiązanych z twoją „oficjalną" tożsamością jak imię, nazwisko, adres, numer

konta. Oczywiście, jeśli posługując się pseudonimową tożsamością użyjesz jakiejś usługi internetowej (maila, Facebooka, Instagrama, Youtube), której kiedykolwiek użyłxś nie maskując numeru IP to także wystarczy. Wspomniany Ross Ulbricht, administrator internetowego sklepu z narkotykami i bronią, popełnił kilka błędów, ale chyba najistotniejszym było to, że w samych początkach swojej działalności zamieścił wpis reklamujący swój ryneczek na jakimś forum internetowym, posługując się swoim adresem na Gmailu. Serio. Później już nie robił aż takich błędów, ale okazało się, że służby dogrzebały się do tego wpisu, który w momencie prowadzenia śledztwa wydawał się już przez wszystkich zapomniany.

Natomiast jest więcej rzeczy, które mogą pomóc cię zidentyfikować lub przynajmniej mocno zawęzić krąg poszukiwań. To np. wyroki i sprawy sądowe jakie dotyczą twojej osoby. Służby rzecz jasna mają takie dane i znane są przypadki identyfikowania osób po sprawach z przeszłości, o których wspominały. Posługując się pseudonimem, nigdy więc nie wspominaj o takich rzeczach. Dość unikatowe mogą być także twoje problemy zdrowotne i leki, które przyjmujesz. Mówienie o filmach, które wczoraj oglądałxś i wydarzeniach kulturalnych, w których brałxś udział, a także o knajpach czy innych biznesach w twojej okolicy z pewnością pomoże cię odszukać. Również wspominanie o pogodzie, jaka była w twojej okolicy w określonym czasie, a już zwłaszcza o takich ultra-lokalnych zjawiskach jak burze, daje dobre wyobrażenie o twojej lokalizacji w danym momencie. Warto też zwrócić uwagę na język jakiego używasz. Należy pisać poprawnie. Możesz pobawić się w stylizowanie swojego języka na żargon jakieś grupy, do której nie należysz. Jeśli dużo różnych osób stylizuje swoją pisownie w określony sposób, to trudniej wychwycić indywidualne cechy w stylu pisania. Możesz używać form gramatycznych właściwych innej płci niż robisz to zwykle, lub nie używać żadnych form nacechowany płciowo. Tak czy inaczej pamiętaj, że twój styl wypowiedzi jest unikatowy i bez żadnych zabiegów także może pomóc cię zidentyfikować.

Wreszcie pamiętaj, że to co cię identyfikuje to także siatka połączeń z innymi osobami. Jeśli w jakiejś działalności używasz określonej tożsamości pseudonimowej, to może się tak zdarzyć, że będziesz współpracować z osobami, których inne tożsamości znasz. Możesz na przykład znać oficjalną tożsamość osoby, która posługuje się w komunikacji z tobą pseudonimem lub inny pseudonim tej osoby. Niemniej, nigdy nie możesz w żaden sposób odnosić się do innych tożsamości takich osób. Niedopuszczalne są takie rzeczy, jak pisane z maila pseudonimowego na „oficjalne” skrzynki pocztowe innych osób, albo na ich skrzynki powiązane z innymi tożsamościami. Nie należy także odnosić się do faktów, pseudonimów itp. powiązanych z innymi tożsamościami. Mam nadzieję, że pamiętasz jeszcze, by nigdy nie rozmawiać o akcjach bezpośrednich. Nawet z tymi ludźmi, z którymi je robiłxś. Zaplanuj akcję, wykonaj, zewaluuj i nigdy więcej się do niej nie odnoś. To taka uwaga na marginesie.

6.6.4. Tryby komunikacji

Można wyróżnić 4 tryby komunikacji w odniesieniu do anonimowości lub pseudonimowości.

1. Anonimowy nadawca, dowolny odbiorca

   Mamy do czynienia z taką sytuacją gdy przekazujesz jakiś komunikat anonimowo i komunikat ten skierowany jest do jakiejkolwiek publiki. Ma to miejsce, gdy piszesz coś na publicznie dostępnym forum używając Tora lub gdy piszesz sprayem po murze.

2. Nadawca i odbiorca znają się nawzajem, ale ukrywają swoje tożsamości przed światem

   To częsty scenariusz w grupach osób anarchistycznych. Zdarza się, że piszemy do naszych znajomych używając anonimizujących narzędzi czy pseudonimów.

3. Działalność niepseudonimowa prowadzona przy pomocy anonimzujących narzędzi

   Może się zdarzyć, że korzystając z jakichś narzędzi anonimizujących - np. Tora lub VPNa - będziesz chcieć się zalogować do jakiejś usługi, która zna twoje prawdziwe dane np. do banku czy mediów społecznościowych. Rzadko ma to sens w naszym kontekście, ale przykładowo w kraju, w którym jakaś usługa jest cenzurowana, może ci się to zdarzyć.

4. Tryb nieanonimowy

   To tryb jaki przyjmujemy, gdy po prostu komunikujemy się używając naszej oficjalnej tożsamości, bez żadnych zabiegów anonimizujących.

Jeśli już umiesz rozpoznać te 4 tryby, to ważne żebyś nigdy ich nie łączyłx w czasie i abyś nigdy nie używałx tych samych narzędzi do nich. Idealnie do osobnych trybów mieć osobne systemy operacyjne, np. do trybów 1 i 2 osobne Tailsy, ale wiem że to może być mało praktyczne, więc przynajmniej użyj wbudowanej w Tor Browser funkcjonalności „Nowa tożsamość". Gdy naciśniesz równocześnie Ctrl + Shift + U to TB wyczyści wszystkie twoje ciasteczka i zalogowania, zamknie wszystkie karty i otworzy zupełnie nową sesję.

6.7. Pseudonimowy mail

Wiele osób tworzenie nowej tożsamości do działań on-line zaczyna od założenia nowej skrzynki e-mail. Niestety, często to konieczne. Wiele usług wciąż wymaga podania maila, lub co gorsza telefonu. Niektórych spraw nie da się załatwić nie mając do danej tożsamości przypisanej ani telefonu ani maila. Tymczasem w dzisiejszych czasach trudno jest założyć e-maila przez Tora nie podając żadnych identyfikujących danych.

Jeszcze do niedawna mali p*scy dostawcy akceptowali zakładanie i sprawdzanie skrzynek przez Tora i nie wymagali podawania numeru telefonu ani alternatywnego maila. Teraz się to zmienia. Warto zawsze przemyśleć czy na 100% mail jest ci konieczny. Możesz założyć konta na niektórych stronach i w niektórych komunikatorach nie podając ani telefonu, ani maila. Jeśli masz opcję nie zakładać maila, nie zakładaj go.

Być może do naszej obecnej działalności wystarczy jednorazowy adres mail, który przestanie działać po kilkunastu minutach. Raczej nic z niego nie wyślesz, ale jeśli chcesz odebrać tylko jedną wiadomość, np. zweryfikować rejestrację konta na jakiejś stronie, to możesz spróbować z taką jednorazową skrzynką email. Niestety wiele stron rozpozna jednorazowego maila i go odrzuci. Dostawców jednorazowych maili jest sporo. Rozsądnie wpisać po prostu w wyszukiwarkę: „One time mail".

Jeśli musisz założyć trwałego maila, to nadal najlepszym wyborem jest założenie skrzynki na mail.riseup.net, oczywiście przez Tora.

Riseup pozostaje jednym z niewielu operatorów maila, który nie wymaga podania deanonimizujących danych, typu numeru telefonu, czy „alternatywnego mail" przy zakładaniu konta. To czyni z niego atrakcyjne narzędzie, ale bynajmniej nie żadne panaceum na wszystkie problemy. Riseup mail działa ładnie przez Tora i ma ogólnie dużo zalet. Pewnie przez najbliższe dziesięciolecia wiele fajnych rzeczy się wydarzy dzięki istnieniu kolektywu Riseup. Problem jest jednak taki, że Riseup będzie od ciebie wymagać podania kodu zaproszenia. Ktoś musi ci to zaproszenie wygenerować, może być to twoja inna tożsamość, ale musisz mieć na uwadze, że Riseup zbiera i przechowuj informacje o tym kto kogo zaprosił. Stworzysz zatem połączenie pomiędzy twoją nową tożsamością, a kontem, które ją zaprosiło.

Chyba powinnxś też wiedzieć, że Riseup w 2016 roku przekazał FBI dane dwóch osób, które korzystały z usług kolektywu i moim zdaniem dość mętnie się z tego wytłumaczył. Nie mówię, że ja zrobiłbym coś lepiej na ich miejscu. Mówię, że nie powinnienxś ufać nikomu, a już na pewno nikomu kogo dobrze nie znasz (i mówię też, że nawet za grube pieniądze nie zapisałxbym się do kolektywu Riseup).

Generalnie warto przyjmować, że Riseup nie jest tym za co się podaje i zachować ostrożność. Jeśli logujesz się przez Tora, to Riseup nie wie kim jesteś. Warto przemyśleć jednak to jakie konto zaprosi twoją nową tożsamość do skorzystania z usług kolektywu.

6.8. Nigdy nie ufaj elektronice 2: możliwości globalnego przeciwnika

Jeśli ostrzeżenia zawarte w rozdziale 3.3. są dla ciebie niewystarczające by trzymać się z dala od elektroniki to pozwolę sobie jeszcze na moment wrócić do tego tematu. W komputerowym opsec jest takie pojęcie jak „globalny przeciwnik". Globalny przeciwnik to osoba, lub grupa osób, która ma możliwość monitorowania wszystkich końców sieci. Agencje wywiadowcze tworzące Sojusz Pięciu Oczu (czyli agencje stanów zjednoczonych amerykkki, kkkanady, a*tralii, nowej z*landii i w*kiej brytanii) są globalnym przeciwnikiem, natomiast podwórkowe p*lskie służby są popychadłami tego przeciwnika. Jeśli przeciwnik monitoruje twoją sieć lokalną i stronę internetową czy usługę, z którą się łączysz, to wie że ty to ty i nie ma znaczenia czy łączysz się przez Tora czy nie.

Jeśli przeciwnik ma dostęp do strony internetowej, z którą się łączysz, np. do forum internetowego na którym nawołujesz do akcji bezpośrednich i widzi kiedy jesteś tam zalogowanx i jednocześnie ma swoich ludzi, którzy sprawdzają kiedy łączysz się do Tora, to na podstawie prostej korelacji czasu będzie wiedzieć, że ty to ty.

A to oznacza, że jeśli znajdziesz się pod obserwacją to się nie ukryjesz. Twoja jedyna szansa to nie rzucić się w oczy i pozostać niezauważonxm. Niech sprawdzają ruch w innym miejscu sieci. Niech stoją pod czyimś innym domem. Niech nie mają powodu by zwrócić na ciebie uwagę.

6.9. Po czym rozpoznać sensowny kanał komunikacji?

Jeśli pomimo licznych ostrzeżeń dotyczących używania elektroniki w ogóle, a już zwłaszcza urządzeń mobilnych, zamierzasz korzystać z cyfrowych urządzeń do szyfrowanej komunikacji, to warto żebyś znałx kryteria po jakich można rozpoznać sensowny sposób komunikacji.

6.9.1 Szyfrowanie end-to-end

Szyfrowanie end-to-end to standard, którego absolutnie nie wolno nam porzucać. Określenie end-to-end oznacza, że wiadomość jest szyfrowana u nadawcy i odszyfrowywana u odbiorcy, pozostając zaszyfrowaną przez całą drogę. Nie jest ona zaszyfrowana tylko na urządzeniach końcowych i na nich może być odczytana. Zdarzają się jeszcze wciąż oszukańcze usługi, które piszą o tym, że są bezpieczne i szyfrowane, podczas gdy nie oferują szyfrowania end-to-end, a jedynie szyfrowanie w przesyle (in transition). W wypadku szyfrowania w przesyle wiadomość jest szyfrowana u nadawcy i odszyfrowywana u pośrednika (np. u dostawcy poczty) i szyfrowana gdy wyrusza w drogę do odbiorcy. Oznacza to, że pracownicy pośrednika i p*icja mają dostęp do treści wiadomości. Przykładem firmy, która oferuje tylko szyfrowanie w przesyle (w większości wypadków) jest Protonmail. Protonmail szyfruje end-to-end tylko komunikację wewnętrzną, pomiędzy jedną skrzynką na protonie a inną.

Wire, Session i Element to komunikatory, które szyfrują end-to-end wszystkie rodzaje wiadomości. Signal umożliwia wysyłanie z aplikacji SMSów, które nie są zaszyfrowane, stosunkowo łatwo więc popełnić głupi błąd używając Signala.

6.9.2. Znikające wiadomości

Im bardziej „efemeryczna” jest wiadomość tym lepiej. Jest już całkiem sporo aplikacji do szyfrowanej komunikacji, które umożliwiają włączenie znikających wiadomości. Jeśli wiadomość znika to nie może być dowodem. Wiadomości są kasowane u nadawcy i u odbiorcy, więc znikają w dwóch punktach, w którym mogą być przechwycone jeśli p*icja w taki czy inny sposób przejmie telefon lub komputer. Czy faktycznie znikają na serwerach

dostawcy usługi tego nie wiemy i sprawdzić nie możemy. Ale jeśli używamy usługi szyfrowanej end-to-end to nieznikniecie wiadomości na serwerze jest najmniejszym problemem, bo wiadomość na serwerze jest zaszyfrowana. Zawsze ustawiaj znikające wiadomości we wszystkich konwersacjach. Im sprawa jest ważniejsza, tym szybciej powinny znikać wiadomości . Session, Wire i Signal oferują znikające wiadomości. Niestety nie ma takiej opcji w Elemencie, co wyklucza go z grona sensownych narzędzi komunikacyjnych, a szkoda, gdyż w przeciwnym razie byłaby to ciekawa aplikacja. W Wire ustawienie znikających wiadomości w czacie 1 na 1 dotyczy tylko wiadomości strony, która je ustawiła, a zatem znikające wiadomości muszą być włączone przez obie strony komunikacji.

6.9.3. Brak powiązania z numerem telefonu i innymi danymi identyfikującymi

Sensowny kanał komunikacji musi wspierać anonimowość. Konieczność podania numeru telefonu lub innych danych identyfikujących jest dyskwalifikująca. Signal, podobnie jak Whatsapp, nie dość że wymaga podania numeru telefonu, to czyni go widocznym dla wszystkich uczestniczek konwersacji, co sprawia, że tworzenie grupy na Signalu jest równoznaczne ze stworzeniem listy imion i nazwisk osób zaangażowanych w jakieś działania. To jest zazwyczaj głupie i raczej powinno być zwalczane. Session i Element nie wymagają podania żadnych danych (w tym maila), co sprawia, że są dodatkowo atrakcyjne. Wire można założyć na numer telefonu lub adres e-mail. Ani numer telefonu ani mail nie są na Wire widoczne dla innych osób.

6.9.4. Wieloplatformowość, w tym możliwość użycia przez Tora

Dobrze jeśli kanał komunikacji nie narzuca rodzaju urządzenia i systemu operacyjnego. To kolejna rzecz, która wyklucza Signala, bowiem pełną funkcjonalność ta aplikacja ma tylko na smartfonie z Androidem lub na iPhonie. Ze wspominanych aplikacji Session i Wire działają dosłownie na wszystkim. Session ma jedną zaletę, która w pewnych okolicznościach staje się wadą. A mianowicie Session wykorzystuje tę samą technologię anonimizacyjną co sieć Tor. To dobrze, ale sprawia to, że nie należy łączyć Session z Torem. Szczegóły techniczne stojące za taką obserwacją są dość skomplikowane. Mówiąc najprościej, twórcy Tora nie zakładali, że ktoś będzie robić coś takiego jak Session, a twórcy Session chcieli zrobić aplikację, która będzie działać anonimowo bez Tora. Oznacza to, że nie powinno używać się Session na systemach operacyjnych, które puszczają cały ruch przez Tora, takich jak Tails. Ten mały mankament trochę utrudnia uznanie Session za idealną aplikację, aczkolwiek pozostaje in ciekawą opcją.

Wire można odpalić na wszystkim, na telefonie, na komputerze z Linuxem, na Macu i na Windowsie. Co krytycznie ważne w naszym wypadku, można go też bez przeszkód używać z Tailsa.

6.9.5. Otwarty kod źródłowy

Dobra aplikacja do komunikacji publikuje kod źródłowy, a także szczegółowy opis swojego działania, a w idealnej sytuacji także wyniki zewnętrznych audytów bezpieczeństwa. Wtedy każda osoba może przyjrzeć się oprogramowaniu w poszukiwaniu błędów i dziur. Session, Wire, Element i Signal spełniają te kryteria. Whatsapp ma zamknięty kod źródłowy co eliminuje go z grona interesujących aplikacji. W Whatsappie może być tylna furtka dla służb specjalnych i nikt nie może tego sprawdzić.

6.9.6. Brak możliwości popełnienia błędu

Współczesne oprogramowanie do szyfrowanej komunikacji jest generalnie łatwe w obsłudze, aczkolwiek zdarzają się niespodzianki. Signal umożliwia wysłanie niezaszyfrowanego smsa do osoby, do której mamy numer, jeśli nie mamy jej dodanej do kontaktów w Signalu. Zdarzało mi się dostawać wrażliwe informacje tym kanałem od osób, które się zagapiły. Wire i Session wymagają minimalnej konfiguracji i praktycznie zerowej wiedzy, są też całkowicie odporne na błąd, gdyż nie obsługują niezaszyfrowanych wiadomości.

6.9.7. Podsumowanie – najlepszy kanał szyfrowanej komunikacji (lato 2022)

Tego typu informacje szybko się dezaktualizują. Podane wyżej kryteria są w miarę ponadczasowe i możesz stosować je samodzielnie. Jeśli zastosujesz je do oprogramowania do szyfrowanej komunikacji dostępnego w lecie 2022 okaże się, że jedyną aplikacją spełniającą wszystkie powyższe kryteria jest Wire. Wire można ewentualnie zastąpić Session, jeśli przyjąć, że ty i twoja grupa korzystacie z urządzeń, które nie przesyłają ruchu przez Tora (czyli nie używacie Tailsa).

Session jest generalnie lepszą i bardziej nowoczesną aplikacją niż Wire, zwłaszcza jeśli chodzi o łatwość obsługi, komfort użycia itp. Niemniej, jeśli już w ogóle korzystać z elektroniki to najlepiej z systemów, które wszystko puszczają przez Tora, czyli najczęściej z Tailsa. Stąd osobiście raczej polecam ludziom Wire.

6.9.8. Zapomnij o szyfrowanych mailach

Paleospecjaliści od opsec twierdzą, że nic nie jest bezpieczniejsze niż szyfrowany mail. Chodzi im o maile szyfrowane za pomocą biblioteki GPG/PGP, czyli takiego małego programiku, który jako pierwszy, wiele lat temu, przyniósł mocną kryptografię pod strzechy. Obecnie najbardziej popularną implementacją tej biblioteki jest program Thunderbird, który umożliwia pozornie łatwe szyfrowanie maili. GPG/PGP bywa też używane przez różne wtyczki do przeglądarek itp. Tymczasem jeśli przyłożyć wcze sniej wspomniane kryteria do GPG/PGP, to wypada słabo, ponosząc porażkę na dwóch polach: znikających wiadomości i braku możliwości popełnienia błędu.

GPG/PGP generalnie przez lata było jedyną powszechnie dostępną opcją szyfrowanych wiadomości i otoczone jest odium „szyfrowania dla tych co się znają". I to prawda, szyfrowanie maili za pomocą Thunderbirda, czy ogólnie za pomocą biblioteki GPG/PGP jest trudne i podatne na błędy. Warto jeszcze dodać, że email zawsze był fatalnym kanałem komunikacji, bardzo źle rozwiązanym z punktu widzenia anonimowości i prywatności. Email powstał jako szybsza alternatywa dla kartki pocztowej, na potrzeby podstarzałych hipisów pracujących w amerykańskich agencjach rządowych i przesyłających sobie pozdrowienia ze stacji badawczych z Antarktydy na Alaskę i z powrotem. Fakt, że ten kanał komunikacji ma lata świetności za sobą, był znany w społeczności zainteresowanej opsec w sieci od przynajmniej dekady. Znikających wiadomości w wypadku maila po prostu nie ma jak zaimplementować i pewnie nigdy się to nie stanie. Od kiedy mamy alternatywy dla maila, można powoli o nim zapominać.

Niemniej, nadal może się zdarzyć, że spotkasz na swojej drodze ludzi, którzy będą chcieli komunikować się wyłącznie szyfrowanymi mailami. Generalnie, jeśli umie się to robić i ma się świadomość tego, że maile zostaną na komputerze drugiej strony potencjalnie na zawsze, to nie jest to zła metoda komunikacji.

7. Case study: zakupy na akcję

Mając już omówione podstawowe zagadnienia związane ze zdalną komunikacją możemy wrócić do konkretów. Z pewnością zdarzy się, że będziesz chciałx kupić jakiś sprzęt lub ubranie specjalnie na akcję.

7.1. Kupuj stacjonarnie!

Oczywiście najlepiej zrobić to w stacjonarnym sklepie, nie wysyłkowo i zapłacić gotówką. Nie należy kupować niczego pod swoim domem. Generalna zasada brzmi, że im bardziej charakterystyczną lub nietypową rzecz kupujesz tym dalej należy to zrobić od swoich zwykłych szlaków komunikacyjnych. Jeśli kupujesz np. gwoździe standardowego rozmiaru lub zwykły spray, to od biedy możesz je kupić w najbliższym markecie budowlanym. Szansa, że zostaniesz zauważonx i tak jest niewielka. Jeśli chcesz natomiast kupić rzadkie odczynniki chemiczne albo np. jakiś kwas, który zostanie znaleziony na miejscu akcji, to lepiej kup to gdzieś daleko od miejsca działań i miejsca własnego zamieszkania. Najlepiej także kupować rzeczy jak najwcześniej, tak by od zakupu do akcji minęło dużo czasu, zwłaszcza w wypadku charakterystycznych przedmiotów. Utrudni to p*icji poszukiwania.

7.2. Wysyłka do paczkomatu i płatność na poczcie

Jeśli nie ma opcji na zakup stacjonarny danego towaru (to rzadka sprawa, mi się jeszcze nie zdarzyło) to możesz od biedy zamówić go do paczkomatu. InPost, główny operator paczkomatów w p*lsce wciąż jeszcze wysyła wszystkie dane potrzebne do odebrania paczki nie tylko na numer telefonu, ale też na maila. Oznacza to, że możesz podać zupełnie lipny numer telefonu (123456789 wygląda głupio, odradzam) i psuedonimowego maila, którego obsługujesz tylko przez Tora. Kod potrzebny do odbioru paczki przyjdzie mailem. Jeśli nie masz pseudonimowego maila, możesz użyć burner phone'a, choć to nastręczy ci dodatkowych problemów z wyjazdami, aby go włączyć i odebrać smsa.

Jeśli zamawiasz coś legalnego to szansa, że paczka będzie śledzona jest bardzo mała. Paczkomaty są jednak skrajnym przykładem miejsca objętego monitoringiem. Odbierając paczkę, pamiętaj o ukryciu charakterystycznych cech twojego wyglądu tak, jak opisałxm w rodziale 3.1.

Aby jednak otrzymać taką paczkę, musisz także jakoś za nią zapłacić. Jeśli sprzedawca podaje numer konta, to możesz to zrobić przelewem zlecanym na poczcie. Polega to na tym, że przychodzisz na pocztę z gotówką i prosisz o zlecenie przelewu na takie to a takie konto. Wypełniasz druczek, podając dane odbiorcy i dane nadawcy, w które wpisujesz cokolwiek. Nigdy nie słyszałxm, by ktokolwiek został przy tej czynności poproszony o dokument. Minusem jest to, że musisz się podpisać, zostaje więc ślad twojego pisma. Tak czy inaczej, warto wybrać małą pocztę, na której nie ma kamer. Można też przyjść w maseczce.

7.3. Zakup „nielegalnych" towarów przez darknet

Inną opcją zdalnej płatności, która może być anonimowa, są kryptowaluty. Większość sprzedawców legalnych towarów i usług nie obsługuje jednak płatności w kryptowalutach. Ale z kryptowalutami będziemy mieć najczęściej do czynienia przy zakupie zupełnie „nielegalnych" towarów.

Zatem, zanim pomyślisz o kryptowalutach, przypomnij sobie to wszystko co pisałxm o elektronice. Weź też pod uwagę, że w darknecie kupujesz od ludzi, którym nie możesz zaufać. Nie wiesz nic o tych osobach, musisz więc założyć, że mogą być z p*icji. Jeśli tak rzeczywiście jest, to znaczy, jeśli kupisz jakąś rzecz od podstawionego p*icjanta, raczej nie uda ci się pozostać na wolności. Jeśli nadawcą twojej paczki jest p*icja, to może ona bez trudu obserwować przesyłkę na każdym etapie jej podróży i być przy tobie w momencie, w którym ją odbierzesz. Niektórzy wykorzystują tak zwane słupy do odbioru paczki, licząc się z tym, że słup może wpaść i pójść do więzienia. Pojawia się jednak wtedy problem tego co „słup" o tobie wie oraz jak uda ci się odebrać od niego paczkę, jeśli jest on pod obserwacją. Z tego powodu nie polecałxbym kupowania w darknecie bardzo wrażliwych towarów. Na popularnym p*skojęzycznym ryneczku przez długie miesiące wystawiona była oferta sprzedaży pistoletu maszynowego. Nie dziwię się, że nie było chętnych.

Paradoksalnie sprzedawanie przez darknet wydaje się bezpieczniejsze niż kupowanie. Sprzedając musisz po prostu dokładnie wyczyścić towar i paczkę z odcisków palców i ewentualnego DNA. Reszta to już nie twój problem.

Jeśli jednak liczysz się z ryzykiem, możesz zamówić przez darknet dostawę „nielegalnego" towaru do paczkomatu, dokładnie tak samo jak wypadku zakupu „legalnego" towaru. Będziesz mieć po prostu trochę więcej stresu przy odbiorze paczki. W darknecie sprzedający będzie od ciebie oczekiwać zapłaty w kryptowalutach (jeśli nie, to raczej jest z p*icji). Teraz pojawia się pytanie, jak anonimowo zdobyć kryptowaluty?

7.3.1. Zakup i anonimizacja kryptowalut

Bitomaty to urządzenia przypominające bankomaty, służące do zakupu i sprzedaży kryptowalut. Na stronie: `https://coinatmradar.com/bitcoin-atm-map/` możesz znaleźć najbliższy bitomat i sprawdzić jakie kryptowaluty on obsługuje.

Jest sporo rodzajów kryptowalut, które niespecjalnie się od siebie różną. Dla ciebie najważniejsze jest, że kryptowaluty dzielą się na takie, które mają stały kurs do dolara lub innej państwowej waluty i takie, których wartość cały czas się zmienia. Ich wartość może spadać lub wzrastać. Kryptowaluty różnią się też wysokością opłat transakcyjnych. Generalnie każda operacja w kryptowalutach coś kosztuje, można to porównać do opłaty za przelew. Najpopularniejsze waluty, Bitcoin (BTC) i Ethereum (ETH), mają ogromne koszty transakcyjne i właściwie zupełnie bez sensu ich używać. Dość łatwo dostępną walutą o niskich kosztach transakcyjnych jest Litecoin (LTC), Litecoin nie ma stałego kursu do dolara, a jego wartość potrafi się dość drastycznie wahać, stąd dobrym pomysłem jest trzymanie pieniędzy w LTC krótko (lub pogodzenie się z ryzykiem kursowym). Coraz bardziej popularną alternatywą dla LTC jest Dogecoin (DOGE).

W miarę popularną walutą, która ma stały kurs do dolara jest Tether (USDT). Tether jest zawsze wart 1 dolara (USD). Stąd jeśli chcesz przechowywać krypto przez dłuższy czas i chcesz mieć pewność, że ich wartość nie spadnie, to kup Tethera. Problem z Tetherem jest taki, że ma wysokie koszty transakcyjne. Więc to dobry sposób na przechowanie pieniędzy, niekoniecznie na ich wydawanie.

Możesz więc w bitomacie kupić Litecoina, Dogecoina lub Tethera, ale i tak celem anonimizacji musisz wymienić zakupioną walutę na Monero (XMR).

Monero to kryptowaluta o zmiennym kursie do dolara i niskich opłatach transakcyjnych. Z grona innych, podobnych walut wyróżnia się tym, że otrzymując płatność w Monero, nie możesz dojść do tego, skąd ona pochodzi. Wszystkie inne krypto są bardzo łatwe do śledzenia. Każda osoba może prześledzić historię wszystkich transakcji, w jakich brały udział określone środki. Przykładowo, jeśli jutro kupisz te swoje Dogecoiny w bitomacie, a potem na coś je wydasz, to ja, wiedząc o tym gdzie je kupiłxś, o której i ile, będę mogłx w nieskończoność śledzić losy tych konkretnych monet, tak jakby przyczepiony był do nich nadajnik. Obsługujesz swoje kryptowaluty przez Tora, więc nie jest z nimi powiązane twoje IP, ale jest powiązany z nimi obraz kamer w bitomacie i w jego okolicy. Natomiast wymieniając kryptowalutę na Monero wkładasz swoje środki do czarnego pudełeczka i trop się urywa.

Pojawiają się już także bitomaty, w których od razu można kupić Monero. To ciekawa opcja, ale póki co uważam, że bardziej ryzykowna. Jest to sposób na zaoszczędzenie paru groszy opłat transakcyjnych i odjęcie sobie pracy z wymianami walut, ale jeśli już masz dać się nagrać na kamery jak kupujesz kryptowaluty, to myślę, że mniej uwagi do siebie przykujesz, jeśli to będzie Dogecoin a nie Monero.

Oczywiście, musisz do tego podejść tak, żeby idealnie nikt się nie dowiedział, że kupiłxś jakiekolwiek kryptowaluty, a już zwłaszcza, że wymieniłxś je na Monero. Aby to zrobić trzeba pójść do bitomatu bez telefonu i w maseczce oraz w czapeczce z daszkiem, a najlepiej także w luźnych ciuchach i w za dużych butach, by mieć zmieniony chód. Tutaj jednak chciałxm zaznaczyć, że operatorzy bitomatów ogólnie są zblatowani z p*icją i coraz częściej bitomaty przypominają twierdze obstawione kamerami. Zdarzają się też nalepki z przekreślonym kapturem i jakieś informacje, że nie można w okularach czy coś takiego. Słyszałxm też o wychodzących z ukrycia ochroniarzach pytających o dowód, jeśli osoba

miała okulary czy kaptur. Mnie nic takiego nie spotkało. Zawsze operuję małymi kwotami w bitomacie (do 1000 PLN), zawsze jestem przynajmniej częściowo zamaskowanx i nigdy nikt nie próbował mnie zatrzymywać. Podejrzewam, że wypłata dużej kwoty w walucie państwowej (czyli sprzedaż krypto) w maseczce i okularach mogłaby być problematyczna. Takie rzeczy się robi, jak się coś ukradnie albo kogoś zabije.

Operacja zakupu kryptowalut w bitomacie wygląda w ten sposób, że musisz wpłacić pieniądze do bitomatu i zeskanować kod QR, który stanowi coś w rodzaju twojego numeru konta z kryptowalutami. To tyle. Aby uzyskać taki „numer konta" musisz zainstalować sobie aplikację do obsługi danej kryptowaluty (czyli tzw. portfel). Oczywiście zrób to koniecznie na Tailsie lub na Qubes OS. Do obsługi Litecoin na Tailsie można wykorzystać program o nazwie Electrum-LTC. Jest do pobrania ze strony swojego producenta w postaci pliku AppImage. Pliki AppImage są fajne, bo nie wymagają żadnej instalacji.

Pod Tailesm wystarczy pobrać taki plik, przenieść go do Persistent Volume i odpalić kliknięciem. Za pierwszym razem trzeba wcześniej kliknąć na niego prawym przyciskiem i w zakładce Uprawnienia wybrać „Zezwól na uruchamianie jako program". Później nie trzeba już tego robić. Tak uruchomiony program poprosi cię o założenie nowego portfela na kryptowaluty, a konfiguracja zajemie ci minutę. Dysponując już aplikacją z założonym portfelem, musisz wygenerować sobie kod QR, który będziesz mogłx zeskanować w bitomacie. Kod generuje się jednym kliknięciem w Electrum-LTC w zakładce Receive (Otrzymaj). Mając wygenerowany kod QR możesz go sobie wydrukować, albo nagrać na jakieś urządzenie, które ma ekran, ale nie ma karty SIM (czytnik ebooków? tablet?) i z tym fantem oraz z pieniędzmi iść do bitomatu. W bitomacie musisz też zdefiniować, ile pieniędzy chcesz przeznaczyć na opłatę transakcyjną. W wypadku LTC czy DOGE to nie są duże kwoty, a im więcej zapłacisz za transakcję tym szybciej krypto będą na twoim portfelu. Zwykle nawet przy niskich opłatach przelew idzie poniżej godziny, ale zdarza się, że może to trwać do doby. Jeśli to dla ciebie za długo, wybierz coś innego niż minimalną proponowaną kwotę.

A zatem: wkładasz pieniądze, skanujesz kod, idziesz do domu i czekasz. To wszystko.

Jak już namierzysz swój pobliski bitomat, możesz poszukać, czy firma nim operująca nie zamieściła na YouTube albo na swojej stronie filmików, pokazujących dokładnie obsługę tej konkretnej maszyny - zwykle to robią.

Gdy już masz kryptowaluty na swoim portfelu wymień je jeszcze na Monero. Do obsługi Monero pod Tailsem nadaje się portfel Feather, który tak samo pobiera się w formie pliku AppImage i obsługuje właściwie tak samo, jak Electrum-LTC. Gdy masz już portfel na Monero, to wejdź sobie przez Tora na stronę do wymiany krypto. Może być to: `https://changenow.io/`

Tam wymienisz dosłownie każdą kryptowalutę na każdą inną. Musisz tylko podać adres swojego portfela w Monero (możesz wkleić kod QR) i po chwili Monero będą na twoim portfelu w Featherze.

Sprzedawcy "nielegalnych" towarów lubią Monero, więc nie powinnxś mieć potrzeby wymieniać ich potem na coś innego. Sprzedawca na pewno chętnie przyjmie pieniądze w Monero. Ale jeśli się okaże, że z jakichś powodów potrzebujesz innej waluty to możesz potem wymieniać Monero na inne waluty. Po prostu nigdy nie używaj tego pierwszego

portfela, na którego wpłacasz pieniądze w bitomacie. Niech on służy tylko do wpłacania pieniędzy w bitomacie. Zawsze potem wymieniaj na Monero, a potem już rób cokolwiek. Jak potrzebujesz przetrzymać środki przez dłuższy czas polecam wymienić z Monero na USDT. Tak powstanie twoje anonimowe, obsługiwane tylko przez Tora konto oszczędnościowe. Pamiętaj też, że generalnie do każdej kryptowaluty potrzebujesz osobnej aplikacji pod swoim Tailsem.

C. D. N. ?

Anarcho-Biblioteka
Dobry pieróg to wywrotowy pieróg

współudział
Pewne rzeczy 2
Edycja techniczna

pl.anarchistlibraries.net